ABSTRACT

Embodiments of the invention authenticate devices and establish secure connections between devices using static Diffie-Hellman key pairs. A first device obtains in a trusted manner a static DH public key of a second device prior to negotiation. The second device negotiates a secure connection to the first device using a shared secret created from the static DH public key, which serves as both a claim on the second device's identity and an encryption key. The static DH public key can be used to establish subsequent secure, authenticated communications sessions.